LA-UR- 08-7484

Approved for public release; distribution is unlimited.

Title:	The No-Cloning Theorem
Author(s):	William K. Wootters and Wojciech H. Zurek
Intended for:	Physics Today

Form 836 (7/06)

The No-Cloning Theorem

William K. Wootters[1] and Wojciech H. Zurek[2]
[1]*Department of Physics, Williams College, Williamstown, MA 01267, USA*
[2]*Theory Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
(Dated: November 14, 2008)

We gather, copy, and distribute information all the time. We make electronic copies and hard copies of electronic files. We make photocopies of the hard copies. And we have strict laws to prevent the unauthorized copying and distribution of information. But in the quantum world the laws of physics themselves impose restrictions on copying: it is impossible to make a perfect copy of an unknown state. This restriction is expressed in the no-cloning theorem.

The principle of superposition is the foundation of quantum mechanics. It says that when two evolving states solve the same Schrödinger equation, any linear combination of the two is also a solution. For this reason, waves from the two slits in the double-slit experiment simply add together to create the familiar interference pattern. As it happens, this basic principle also prohibits the arbitrary copying of quantum states.

LINEARITY, UNITARITY, AND CLONING

To see why, imagine a machine that copies the state of a photon or an electron. When the original enters, two copies come out, each having the same state as the original. If such a machine were successful, it would convert the state $|\diamondsuit\rangle$ to $|\diamondsuit\diamondsuit\rangle$, and $|\heartsuit\rangle$ to $|\heartsuit\heartsuit\rangle$. (We use arbitrary symbols to represent arbitrary states.) The problem arises when one tries to send their linear combination, $|s\rangle = a|\diamondsuit\rangle + b|\heartsuit\rangle$, through our hypothetical cloner. If $|\diamondsuit\rangle$ and $|\heartsuit\rangle$ are cloned correctly, then because of the linearity of quantum mechanics, the output for their superposition must be the superposition of the outputs, $|e\rangle = a|\diamondsuit\diamondsuit\rangle + b|\heartsuit\heartsuit\rangle$. But we wanted $|s\rangle|s\rangle = (a|\diamondsuit\rangle + b|\heartsuit\rangle)(a|\diamondsuit\rangle + b|\heartsuit\rangle)$, the original and a copy of $|s\rangle$. This is not the state $|e\rangle$ we got!

The difficulty stems from the inherent nonlinearity of copying: When one asks for "two of the same", a *square* $|s\rangle|s\rangle$ of the original $|s\rangle$ is desired. This sets up a conflict with the strict linearity of quantum theory. As a result, a single cloner cannot make a perfect copy of *every* quantum state. So what states can it clone?

So far, we have relied on linearity. But quantum evolutions preserve probability. Thus, the norm $\langle e|e\rangle$ of the state emerging from the copier must be the same as $\langle s|s\rangle$ of the original. The only difference between these two scalar products, expressed in terms of $|\diamondsuit\rangle$ and $|\heartsuit\rangle$, is in the cross term. Thus, the equation $\langle\heartsuit|\diamondsuit\rangle = \langle\heartsuit|\diamondsuit\rangle^2$ must be satisfied by any two states that are perfectly copied. This simple equation has profound consequences: it shows that a quantum copier can work only when the possibilities for the original are orthogonal—$\langle\heartsuit|\diamondsuit\rangle = 0$. We could have also arrived at this conclusion by recognizing that quantum evolutions are unitary—they preserve the scalar product of any two states. So, for states that can be copied we get again $\langle\heartsuit|\diamondsuit\rangle = \langle\heartsuit|\diamondsuit\rangle^2$. This is no surprise; unitarity is a consequence of linearity *and* preservation of the norm.

Quantum evolutions are reversible, so one can imagine running the copier "in reverse", to delete the extra copy in states such as $|\diamondsuit\diamondsuit\rangle$ or $|\heartsuit\heartsuit\rangle$. Uncopying preserves the scalar product, so the simple equation above still applies. It follows that perfect copying or deleting is possible only for sets of states that are orthogonal.

Our initial optimistic assumption that the copier will work "according to specs" for arbitrary $|\diamondsuit\rangle$ and $|\heartsuit\rangle$ was naive. It can be met only when the two states are orthogonal, and even then one can copy *these* two states (and, possibly, their "orthogonal friends") only with a copier that works for this set of states. Thus, for example, one can design a copier for any *orthogonal* pair of polarization states of a photon, but a copier that works for $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ will fail for $\{|\nearrow\rangle, |\nwarrow\rangle\}$, and *vice versa*.

We conclude that one cannot make a perfect copy of an unknown quantum state, as, without prior knowledge, it is impossible to select the right copier for the job. This is a common way of stating the no-cloning theorem.

QUANTUM CRYPTOGRAPHY

While the impossibility of cloning may seem at first an annoying restriction, it can also be used to one's advantage. For instance, in the Bennett-Brassard quantum key distribution scheme, the sender, Alice, transmits many photons to the receiver, Bob, with the aim of ultimately creating a shared, secret, random string of zeros and ones. Such a random string can later be used as a key for encrypting and decrypting messages. In this particular scheme, each of Alice's photons is prepared at random in one of four possible polarization states: vertical, horizontal, +45°, and −45°. An eavesdropper, Eve, would like to get a copy of each photon for herself, but she also wants to pass an accurate copy on to Bob, or else her presence will be detected later when Alice and Bob check a random sample of their results. (They are checking specifically to see if Eve has disturbed their signals.) Notice, though, that—because of the no-cloning

theorem—Eve cannot succeed in this task. As we have just seen, if her cloning device can successfully copy the vertical and horizontal polarizations, it will fail to copy faithfully either of the two diagonal polarizations. Thus the prohibition against cloning is a feature of the world that helps us preserve privacy.

COPYING, CAUSALITY, AND COLLAPSE

If cloning *were* possible, one could communicate instantaneously over a distance. Suppose Alice and Bob share two photons in the entangled polarization state, $|\varsigma\rangle \propto |\leftrightarrow\updownarrow\rangle - |\updownarrow\leftrightarrow\rangle$, a state that can be created, for example, by downconversion. The state $|\varsigma\rangle$ can be expressed in any orthogonal basis, e.g., $|\varsigma\rangle \propto |\nearrow\nwarrow\rangle - |\nwarrow\nearrow\rangle$; twins are always oriented along perpendicular axes. So to try to send information to Bob, Alice might measure her twin in one of two bases, $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ or $\{|\nearrow\rangle, |\nwarrow\rangle\}$, in hopes that her choice of basis will make a difference at Bob's end. Alice's measurement collapses $|\varsigma\rangle$ into one of the states of the basis she chooses. So if she chooses $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$, Bob's photon will end up in one of the two states $|\leftrightarrow\rangle$ or $|\updownarrow\rangle$, whereas if she makes the other choice, Bob's photon will end up in one of the diagonal states.

But Bob cannot read this message: a quantum state cannot be "found out" unless one knows what to look for. The simple question, "What's your state?" is against the rules. A quantum measurement is a multiple choice test. It poses questions such as, "Are you $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$?" Eigenstates of the measured observable are the only admissible answers. If Bob measures the wrong observable he randomizes the state of his twin, erasing Alice's message.

Direct measurements don't work, but what if Bob were to clone his twin first? Copying $\updownarrow$ or $\nearrow$ into $\updownarrow\updownarrow\updownarrow\ldots$ or $\nearrow\nearrow\nearrow\ldots$ introduces redundancy, allowing for error correction. Even a "wrong measurement" on some of the copies would not erase Alice's message, as there are other copies to ask the complementary question. And the right question leads to a consensus—all copies give the same answer in the multiple choice test.

So, perfect copying of unknown states would allow superluminal communication, threatening causality. The no-cloning theorem precludes this. But what happens if Bob uses a more limited copier, a copier, say, just for the basis $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$? If Alice happens to choose that basis, the copier works. If she chooses the other basis, the copier produces a state proportional either to $|\updownarrow\updownarrow\updownarrow\ldots\rangle + |\leftrightarrow\leftrightarrow\leftrightarrow\ldots\rangle$ or to $|\updownarrow\updownarrow\updownarrow\ldots\rangle - |\leftrightarrow\leftrightarrow\leftrightarrow\ldots\rangle$. But an equal mixture of these two states is, unfortunately for Bob, indistinguishable from an equal mixture of $|\updownarrow\updownarrow\updownarrow\ldots\rangle$ and $|\leftrightarrow\leftrightarrow\leftrightarrow\ldots\rangle$. (In fact, each of the complicated states by itself is already difficult to distinguish from such a mixture.) So this kind of redundancy is of no use for communication. The redundancy is nevertheless of interest, as it sheds light on the nature of quantum measurements. Our copier acts as an amplifier: it is restricted to a preferred basis, in consonance with the fact that a quantum measurement is a multiple choice test.

Analogies between a measuring apparatus and a copier are suggestive. Both impose their own choice of preferred states on the preexisting state of the system. Only states that respect this "symmetry breaking" can be found out or copied. Other states are converted into superpositions of redundant branches. In the end, an entangled state that emerges at the output of the device is difficult to distinguish from their mixture.

APPROXIMATE CLONING

If the exact cloning of arbitrary states is impossible, to what extent is it possible to clone states *approximately*? Assuming that the cloner handles all input states equally well and makes two equally good copies in every case, the answer to this question is known: for a two-state system, each clone, if subjected to a test to see if it matches the initial state, will at best pass the test with probability 5/6. (It is interesting that if the fidelity were any better one could use the approximate cloner, together with entanglement, to transmit signals faster than light!) One *can* do better (without admitting superluminal communication) if one tailors the cloning device to a more limited set of states. For example, if one wants to clone only *linear* polarization states, and not circular or elliptical polarizations, the optimal fidelity allowed by quantum mechanics is $1/2 + 1/\sqrt{8} = 0.85$. Only linear polarizations are used in the Bennett-Brassard scheme, and indeed, a strategy based on the optimal cloning of linear polarizations is one of the best ways to eavesdrop against that scheme.

Approximate cloning devices constructed in the lab have come close to acheiving the optimal values of the fidelity, but with a limited probability of success on any given trial. In some cases the experiments are based on linear optics, with success being conditioned on specific measurement outcomes. Other experiments are based on nonlinear downconversion, in which a strong laser pulse facilitates the approximate cloning of a single photon.

The more one restricts the set of possible states, the better chance one has of producing a faithful clone. The ultimate restriction, for the purpose of cloning, is to limit oneself to a set of mutually orthogonal states. As we have seen, this is the only case in which the cloning can be perfect. And this possibility explains why the cloning of a sheep, for example, or the everyday operation of a photocopier, does not violate the no-cloning theorem.

No one is shocked to learn that quantum mechanics does not permit faster-than-light communication. Somehow quantum mechanics "knows" that it should restrict access to information. But it is interesting to see exactly how nature manages to enforce this prohibition. The no-

cloning theorem provides a glimpse into its methods.

Further Reading

V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, "Quantum cloning," Rev. Mod. Phys. **77**, 1225–1256 (2005).

N. J. Cerf and J. Fiurasek, "Optical Quantum Cloning—A Review," Progress in Optics, **49**, 455 (2006).